



增强混合云安全性

利用云原生安全方法来保护您的业务

作者：Lucy Huh Kerner，红帽资深首席安全全球技术宣讲人和战略师

目录

部署安全至上的混合云

如今，94% 的组织使用某种类型的云，58% 的企业采用混合云战略[1]。混合云是一种 IT 架构，它在两个或多个互联但独立的环境中整合了一定程度的工作负载可移植性、编排和管理，包括裸机、虚拟化、私有云和公共云。借助混合云架构，您可以在任何互联环境中运行工作负载，在环境之间移动工作负载，并交替使用这些环境中的资源。

企业采用混合云环境来：

- 连接来自不同供应商的基础架构、平台、应用和工具。
- 提高效率和可扩展性。
- 降低成本。
- 提升敏捷性。
- 优化数据放置。

不管您处于混合云之旅的哪个阶段，安全是重中之重。事实上，81% 的企业认为云安全性是个挑战[1]。混合云安全漏洞通常表现为资源监督和控制丧失，包括未经批准的公共云使用、资源缺乏可见性、变更控制不足、配置管理不善和访问控制无效。未经授权的用户可以利用这些漏洞来访问敏感数据和内部资源。

安全漏洞可能会造成巨大损失。数据泄露的平均成本为 392 万美元，其中业务损失占该成本的 36.2%[2]。威胁还在不断加剧。两年内发生泄露的可能性为 29.6%[2]。2019 年，数据记录的平均数量以及识别和控制泄露的时间均有所增加[2]。

即使面临众多挑战，您还是可以参照本地与云架构之间的区别调整您的方法，从而部署**安全至上的混合云**。本电子书讨论了在混合云中保护您业务的新方法和注意事项。

无效安全防护的影响

安全漏洞可能会造成巨大损失，威胁还在不断加剧。

392 万美元
2019 年数据泄露平均成本[2]。

279 天
2019 年识别和控制数据泄露平均用时[2]。

122 万美元
识别和控制泄露后的成本节约
200 天
或更少[2]。

29.6%
两年内遭遇数据泄露的概率[2]。

1 Flextera：“Flexera RightScale 2019 年度云现状报告”，2019 年 2 月。info.flexerasoftware.com/SLO-WP-State-of-the-Cloud-2019。
2 IBM Security，“2019 年数据泄露成本报告”，2019 年。ibm.com/security/data-breach。

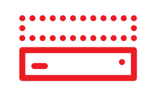


安全是一种流程，而不是产品

有效的安全需要一种能够整合人员、流程和技术的全面方法。仅仅部署以安全为中心的产品和工具并不足以保护您的基础架构、云或业务。您还必须实施安全策略和流程，以利用您的产品功能有效降低安全风险。随着技术、威胁和需求的发展，这些策略和流程必须随着时间的推移进行调整。

混合云环境要求您转变安全方法。因为它们没有定义的边界，基于边界的传统安全方法是无效的。集中式身份管理和访问控制是以云为中心的安全方法的关键。有效的集中式身份管理和访问控制使用最小特权原则，仅向用户提供他们实际需要的访问权限。这种方法需要审核每个用户的当前访问权限，然后重新评估每个用户以确定正确的访问级别。

混合云安全还要求多层次深度防御安全防护策略能够结合环境中每一层的功能，包括操作系统、容器平台、自动化工具、软件即服务（SaaS）资产和云服务。



操作系统

寻找可帮助您确保安全合规、实施物理安全、提高网络安全、控制用户访问、隔离进程和提高数据安全的内置工具。示例包括 OpenSCAP、USBGuard、防火墙、安全增强型 Linux®（SELinux）、身份管理和网络绑定磁盘加密。



容器平台

使用平台和 Kubernetes 中的内置功能来提高容器安全性。示例包括容器集安全策略、网络流量控制、集群入口和出口控制、基于角色的访问控制（RBAC）、集成证书管理和网络微分段。



自动化工具

选择企业中每个人都可以轻松学习和使用的自动化语言，包括开发、运维、安全和合规团队。寻求访问控制、日志记录和审计功能。有关自动化的更多信息，请参见**第 4 页**。

最后，您应该重新考虑现有的安全流程和工具。确保您正在使用所有可用功能，并确定是否可以修改或重新配置任何设置以提供更好的保护，或者是否需要新的流程和工具。

1. 创建当前 IT 资产和工具的清单。
2. 记录您现有的安全和网络架构、网络安全政策、工作流程以及技能和人才缺口。
3. 建立威胁模型并确定您对网络安全漏洞的风险容忍度和缓解策略。
4. 评估您的架构、策略和流程，以确定需要更改的方面。
5. 评估您当前的工具和资产，确定它们是否可以支持您更新的策略和流程。记录并计划如何解决安全漏洞。

以下部分讨论了混合云安全性的关键注意事项，并提供了改进保护的提示。



协作

重要意义

分割式安全方法通常会导致安全漏洞和重复工作，因为安全成为应用开发和基础架构部署中的事后补救措施。随着开发速度和部署灵活性的提高，在流程中尽早考虑安全性变得越来越重要。仅在开发周期结束时应用有效的安全性需要大量时间，这可能导致交付延迟并导致团队无法提供足够的安全性。

建议和最佳实践

使用 DevSecOps 方法统一整个企业的安全性。DevSecOps 是一个协作性框架，其中安全是需要全程关注的共担责任。它将安全性扩展到所有团队，而不是让一个独立的、不相干的团队负责设置安全策略。安全、开发和运维团队的员工携手合作，共享可见性、反馈、经验教训和见解。这种方法允许从开始开发应用和部署基础架构时就集成安全防护，以增强保护。

正式的培训计划可帮助每个人了解安全防护的重要性以及它们如何帮助保护您的企业。 这些计划应该解决以下问题：

- 保持应用和资源符合安全策略和法规。
- 为传统、容器化和混合云环境建立不同的安全防护方法。
- 创建修补策略，帮助您及时了解新的和已有的安全漏洞。

高管支持也很重要。高管应该鼓励协作，并接纳来自整个企业的团队的反馈。



战术步骤

尝试这些操作以增加企业内的协作。

从细节着手，开始发展。

选择一个项目开始。鼓励实验和迭代、持续改进来调整和优化您的流程。庆祝成功并向企业内的其他人展示已证明的价值。

协商设定明确的目标和时间表。

透明度对于 DevSecOps 来说至关重要。确保参与的每个人都理解并同意项目的目标和时间表。

对员工进行交叉培训。

建立有关安全、基础架构和开发的学习路径，这些学习路径会定期更新并随时可供所有团队成员使用。

创建安全工作组。

建立一个集成的跨学科团队来定义安全用例和策略。

向他人学习。

利用美国国家税务局和国土安全部等其他组织的调查结果。



自动化

重要意义

错误配置和不充分的变更控制是对安全的最大威胁[3]。错误配置可能使系统容易受到攻击。变更控制对于了解谁修改了配置、何时修改以及在整个系统生命周期中更改了哪些内容至关重要。自动化可以帮助您简化日常运维，并从一开始就将安全防护集成到流程、应用和基础架构中。实际上，通过全面部署安全自动化，可以让因泄露而造成的平均损失降低 95%，但只有 16% 的企业已经做到这一点[4]。

建议和最佳实践

实施统一的自动化策略，以降低整个企业的错误配置和人为错误的风险。自动化简化并提高了基础架构管理、应用开发和安全运维的一致性，以改进保护、合规性和变更控制。

- 根据预先批准的策略始终如一地配置资源，并在其生命周期内以可重复的方式主动维护资源。
- 快速识别需要补丁或重新配置的系统。
- 根据定义的基线，以一致的方式跨大量系统更轻松地应用补丁或更改系统设置。
- 通过自动记录的操作日志简化审计和故障排除。

为您的自动化平台和流程实施身份管理和访问控制，有助于确保只有授权人员才能执行自动化任务。

选择企业中每个人都可以使用的自动化平台。实现通用、易于学习的自动化语言的平台可以改善：

- **可见性。**每个人都可以理解每个自动化任务的作用。
- **可重复性。**可访问的平台和语言允许所有获得批准的员工有效且高效地使用自动化。
- **相互协作。**自动化任务可以在您的企业中共享，允许其他团队利用已完成的工作并避免重复工作。
- **审计。**多名员工可以验证自动化任务并查看日志以进行审计。

战术步骤

尝试这些操作以开始实施安全自动化。

从单个项目开始。

不要试图立马实现全面自动化。选择单个项目或有限数量的任务开始。

选择重复性任务。

自动执行重复性任务，包括配置管理、软件包和补丁管理、安全漏洞识别和修复以及策略实施。

测量、调整和重复。

以迭代方式部署自动化、衡量结果并进行相应调整。

计划进行扩展。

确保所有自动化都是可验证、可审计和可共享的，以便企业内的其他人可以利用这些优势。



3 云安全联盟，*“云计算的主要威胁：Egregious 11”，2019 年 8 月。*cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven。

4 IBM Security，*“2019 年数据泄露成本报告”，2019 年。*ibm.com/security/data-breach。



更新和补丁

重要意义

未打补丁和过时的系统可能是合规性问题和安全漏洞的根源。事实上，大多数被利用的漏洞都是安全和 IT 团队在发生泄露时已经知道的漏洞。

建议和最佳实践

经常安装补丁并测试您的补丁，确保它们应用正确。每天扫描系统以查找需要修补的合规性问题和安全漏洞。根据您的威胁模型以及风险、性能和时间考量，确定纠正行动的优先级。定期修补所有适用的系统，与重要问题保持同步。尽快为关键问题和已知漏洞应用补丁。将安装了补丁的系统重新投入使用之前，确保对其进行功能测试。

您还应该更新您的修补策略，以考虑从基础镜像部署的云和容器化资源。确保基础镜像符合您企业的安全基线。与物理和虚拟化系统一样，定期扫描和修补您的基础镜像。修补基础镜像时，基于该镜像重建和重新部署所有容器和云资源。

最后，应用自动化来简化修补操作。创建用于修补的自动化工作流，以加快操作、降低错误风险并提高跨系统的一致性。例如，您可以为应用和基础架构使用基于 Jenkins 的持续集成/持续部署（CI/CD）管道，以实现生命周期流程自动化，例如修补。

战术步骤

遵照以下步骤创建更强大的修补和更新策略。

1. 确定需要修补的系统。
2. 根据您的威胁模型、预期风险、性能影响和可用修补窗口确定操作的优先级。
3. 自动应用补丁以提高传统和混合云基础架构的一致性和可重复性。
4. 定期重新评估和调整您的修补策略，与不断发展的功能、技术和威胁同步。



开源技术

重要意义

开源技术是云和容器操作不可或缺的一部分，但如果您的企业使用未签名的软件或以不安全的方式部署这些技术，它们可能会成为安全漏洞的根源。直接使用来自上游社区、未经审查的开源软件可能会让您面临安全漏洞和供应链攻击，这些攻击利用第三方服务和软件的弱点来危害最终目标。这些攻击有多种形式，包括劫持软件更新和将恶意代码注入合法软件。2018 年，供应链攻击增加了 78%[5]。

建议和最佳实践

确保您了解谁分发您使用的开源技术并以安全的方式部署这些技术。首先，盘点您的企业当前使用的开源技术。停止使用任何不是从已知、受信任的来源获得的技术。定义流程和策略，将剩余技术重新归于 IT 和安全团队控制。

您还应该制定以安全为重点的开源技术使用策略。您的策略应包括确保您的开源技术来自可靠来源、以自动化方式不断修补并在配置时考虑到安全防护的措施。此外，您应该鼓励使用企业级开源产品，包括贯穿其整个生命周期的企业支持。



78% 2018 年发生的供应链攻击较上一年增幅[5]。

战术步骤

尝试这些操作来提高您使用的开源技术的安全性。

切换为商用版本。

将您使用的直接来自于上游开源项目的开源软件迁移到受信任的**商用版本**。这些版本经过测试和验证，可降低错误和安全漏洞的风险。它们可能还包括企业支持，可以快速提供安全补丁并提供有关配置软件安全的指导。

阅读**本文**，了解有关安全开源技术的更多信息。

基于模板部署开源软件。

检查您的管理和平台工具，了解它们是否提供基于预定义、经过审查的模板的自助服务置备。您可以使用模板来确保只部署受信任的最新开源技术。快速、自动化的部署还鼓励用户使用授权的 IT 资源，而不是部署 IT 和安全团队无法控制的资源。



5 Symantec，*“互联网安全威胁报告，第 24 卷”，2019 年 2 月。*

准备好开始了吗？

混合云安全是所有企业关注的重要问题。无论您处于混合云之旅的哪个阶段，红帽都可以帮助您部署安全至上的混合云。凭借集成的内置安全功能，红帽的生产级开源软件产品组合为您提供了克服当前和未来安全与合规挑战的工具和平台。红帽还提供企业级支持、实践培训和专家服务，帮助您更高效、更安全地构建和运维混合云环境。

阅读这些资源，了解有关红帽安全性和合规性方法的更多信息。

- **混合云安全防护概述**
- **为什么选用红帽技术来打造 IT 防护**
- **实现安全防护与合规自动化的原因**
- **红帽® 服务：实现系统安全防护与合规自动化**

免费的业务探讨预约，请访问：
redhat.com/zh/services/consulting

Lucy Huh Kerner 是红帽资深首席安全全球技术宣讲人和战略师

Lucy Huh Kerner 帮助培养安全思想领导力，并领导全球整个红帽产品组合的安全技术和上市战略。此外，她还帮助创建安全相关技术内容，并提供给现场、客户、合作伙伴、分析师和媒体，还在众多活动中发表演讲。在担任此职务之前，她是红帽北美公共部门团队的资深云解决方案架构师。凭借她在云技术领域的专业知识，她为北美公共部门众多客户设计和展示红帽云解决方案，以支持红帽云销售工作。Lucy 拥有超过 15 年的软件和硬件开发工程师和售前解决方案架构师的专业经验，工作曾涉及网络安全的各方面。

F18867_0220_KVM

